A Framework of Opportunity-Reducing Techniques to Mitigate the Insider Threat: Towards Best Practice

Keshnee Padayachee

**Abstract**— This paper presents a unified framework derived from extant opportunity-reducing techniques employed to mitigate the insider threat leveraging best practices. Although both motive and opportunity are required to commit maleficence, this paper focuses on the concept of opportunity. Opportunity is more tangible than motive; hence, it is more pragmatic to reflect on opportunity-reducing measures. Opportunity theories from the field of criminology are considered to this end. The derived framework highlights several areas of research and may assist organizations in implementing controls that are situationally appropriate to mitigate insider threat.

**Index Terms**— Abuse and crime involving computers, Network-level security and protection, Organizational management and coordination, Security and Privacy Protection

xxxx-xxxx/0x/$xx.00 © 200x IEEE Published by the IEEE Computer Society

————————————————

1. Keshnee Padayachee is with Institute of Science and Technology Education, University South Africa, South Africa, UNISA, 0003.
2. E-mail:padayk@unisa.ac.za

—————————— ◆ ——————————

# 1 Introduction,

A

ccording to the CyberSecurity Watch Survey [[1](#_ENREF_1)], 46% of the respondents considered the maleficence caused by insider attacks as more damaging than those caused by outsider attacks. The Boardroom Cyber Watch 2013 [[2](#_ENREF_2)] survey in fact cautioned that this estimation may be more than 50%. An ‘insider’ is any individual who has legitimate access to an organisation’s information technology (IT) infrastructure [[3](#_ENREF_3)] while an ‘insider threat’ uses the authority granted to him/her for illegitimate gain [[4](#_ENREF_4)]. The insider threat involves more than a disgruntled employee; it may also include insiders who no longer work for the company but whose system credentials are still valid, or it may include a system developer who has in-depth knowledge of the system [[5](#_ENREF_5)]. Chinchani et al. [[6](#_ENREF_6)] argue that several challenges are associated with the insider threat and claim that security administrators consider the insider threat as unpreventable. Insiders have a higher success rate with maleficence not only because they are familiar with security controls, but also because most tools are aimed at neutralising external threats. Examples of attacks include unauthorised extraction, duplication or exfiltration of data, tampering with data, deletion of critical assets, etc. [[7](#_ENREF_7)]. The motivations of malicious insiders range from apathy to espionage, sabotage, terrorism, embezzlement, extortion, bribery, corruption and ignorance [[8](#_ENREF_8)]. According to Cornish and Clarke [[9](#_ENREF_9)], both motivation and opportunity play a critical role in crime; however, opportunity may be the ‘trigger’ to committing a crime.

According to Theoharidou et al. [[10](#_ENREF_10)] the insider threat issue may benefit from a ‘pluralistic approach’ that would be enriched by ideas from well-established criminology theories. Many theories of crime have their basis in either sociology, psychology or biology; hence, they consider the motivations for crime and attempt to understand why criminals commit crime. Opportunity theories of crime, on the other hand, focus on opportunities that have to be present in order for crime to occur. Motivations are difficult to analyse as they are based on human emotions. In contrast, it is easier to conceptualise opportunities and consequently to develop pragmatic strategies to minimise crime. Felson and Clarke [[11](#_ENREF_11)] indicate that, unlike other factors that may be associated with crime, opportunity is the ‘root cause’ of all crime. It is evident that while one may have the motivation or capability, there has to be an opportunity to commit the crime.

Four theories of crime embody the opportunity theory perspective, namely Rational Choice theory (a dominant theory in economics) [[12](#_ENREF_12)], Routine Activities theory [[13](#_ENREF_13)], Crime Pattern theory [[14](#_ENREF_14)] and more recently Situational Crime Prevention theory [[15](#_ENREF_15)]. Becker [[16](#_ENREF_16)] first identified the relationship between rational choices and crime. He postulated that some individuals are criminals not because ‘their basic motivation differs from that of other persons, but because their benefits and cost differ’. Recently there has been a trend towards using the theory of Rational Choice to explain the insider threat (see [[17](#_ENREF_17)] and [[18](#_ENREF_18)]). Whereas Rational Choice theory is focused on the individual, Routine Activities theory gives more attention to society at large [[11](#_ENREF_11)]. The latter theory is based on the convergence of three elements to explain why crime occurs: motivated offenders, suitable targets, and the absence of capable guardians in time and space [[13](#_ENREF_13)]. Crime Pattern theory in turn is concerned with the spatial and temporal distribution of crime and seeks to detect ‘patterns both in criminal events and for criminals that are scale independent’ [[14](#_ENREF_14)]. The premise is that crime is not random but clustered. Here the issue is ‘to discover and prevent opportunities for crime in the daily commute and other patterns of movement of potential offenders’ [[19](#_ENREF_19)]. Situational Crime Prevention theory (which is based on Routine Activities and Rational Choice theories) asserts that the opportunities for crime should be reduced [[9](#_ENREF_9)]. This theory has been applied to the insider threat (see [[20-22](#_ENREF_20)]) and to general information security concerns (see [[23](#_ENREF_23)] and [[24](#_ENREF_24)])

According to Willison [[20](#_ENREF_20)], it is valuable for researchers to consider computer crimes in terms of criminology theories, as they are, after all, crimes. Theoharidou et al. [[10](#_ENREF_10)] also assert that criminology theories would enrich the current arsenal of information security countermeasures that appear to be derivatives of General Deterrence theory. According to Willison [[20](#_ENREF_20)], both Situational Crime Prevention and Rational Choice theories are highly appropriate to understanding insider threats. Willison [[20](#_ENREF_20)] proposes that the techniques advocated by Situational Crime Prevention theory could reasonably be adopted by information security practitioners. However, it has been argued that the spatial and temporal elements of Crime Pattern and Routine Activities theories are difficult to apply within the cybercrime landscape (see [[25](#_ENREF_25)] and [[19](#_ENREF_19)]). This discrepancy provides a significant potential for further research within the cyber security domain and highlights a secondary aim of the framework, namely to identify research gaps between opportunity theories and their application to cybercrime.

An effort is made in this study to derive a framework that may be used to develop a unified strategy to mitigate the insider threat and to identify areas of potential research. The framework combines a benchmark of best practices with the formal description of situational crime prevention. The objective of this research is to determine the extent to which Situational Crime Prevention satisfies the principles of best practices for insider threat mitigation. The rest of the paper is structured as follows: Section 2 amplifies the definition of the insider threat while Section 3 presents related work on the traditional mechanisms deployed to manage the insider threat. The role of opportunity with regard to mitigating the insider threat is elaborated on, in Section 4. Section 5 evaluates the current status of opportunity-reducing techniques. Section 6 presents a discussion on the findings and the paper concludes with Section 7.

# 2. Delineating The Insider Threat

An essential difference between outsiders and insiders is that outsiders have limited opportunity to carry out their attack. The latter have to exploit vulnerabilities in the system, while insiders have privileged access and hence greater opportunity [[26](#_ENREF_26)]. Insiders have a significant advantage as they do not only have knowledge about vulnerabilities in policies, networks or systems [[27](#_ENREF_27)], but also the requisite capability. Walton [[26](#_ENREF_26)] observes, on a positive note, that the insider (unlike an outsider) is subjected to policies, procedures and agreements. For instance, if an insider agrees to be subject to monitoring by a honeypot, then unlike an outsider he/she may have no legal recourse. An insider has ‘legitimate access to an organisation’s computers and networks’, while an insider threat is an entity that places organisations’ assets at risk [[28](#_ENREF_28)]. Bishop and Gates [[29](#_ENREF_29)] further qualify the modus operandi of the insider threat as constituting a violation of information security policy using either authorised access or unauthorised access. There are two classes of insider threats: traitors and masqueraders. Traitors are legitimate users that abuse their privileges and masqueraders are insiders that impersonate other users for malicious purposes [[30](#_ENREF_30)].

Bowen et al. [[31](#_ENREF_31)] recommend that decoys be designed with the following levels of sophistication that characterise the insider threat: However, these characterisations apply in general:

* **Low**: This type of insider relies on what may be discerned from a cursory scan such as shoulder surfing.
* **Medium**: This type of insider performs verifications from other sources to check the authenticity of the information, for example by using a search engine.
* **High**: This type of adversary has access to the most sophisticated tools, for example key stroke loggers.
* **Highly privileged**: This type of adversary may know that there are decoys or detection systems and will attempt to disable or avoid them.

Sophisticated users are more dangerous as they are more likely to cause detrimental attacks and able to cover their tracks more effectively [[32](#_ENREF_32)]. However, it may be prudent to monitor those insiders with higher privileges more closely. Furthermore, a highly sophisticated insider may be able to identify and exploit opportunities more successfully than would a less sophisticated user.

Wood [[33](#_ENREF_33)] describes the attributes of an insider threat as access, knowledge, privileges, skill, risk, tactics, motivation and process. An insider has ‘unfettered’ access to parts of a system and he/she may even have privileged access [[33](#_ENREF_33)]. An insider’s tactics are based on his/her goals, and the process describes the stages that lead the insider to commit maleficence [[33](#_ENREF_33)]. The process ranges from the intrinsic motivation of the insider, to identifying a target, to planning and finally launching the attack [[33](#_ENREF_33)]. The propensity for risk and the motivation factors are intrinsic to the insider. The knowledge and skills factors are related to the particular insider’s capability. It is clear that insiders require the knowledge and skills to commit maleficence. However, an insider’s privileges and access rights may further embolden him/her to consider crime. For example, an insider who has access rights to confidential information has a greater opportunity to commit crime. Hence controlling the granularity of access may be an opportunity-reducing measure.

The insider threat will become even more insidious with the general adoption of cloud computing and the ubiquity of social networking. From a cloud computing perspective, the concept of the insider is multi-contextual. It ranges from the rogue administrator of a cloud service to an insider ‘who uses cloud systems to carry out an attack on an employer’s local resources’ [[34](#_ENREF_34)]. Molok et al. [[35](#_ENREF_35)] maintain that social networking has caused damages to organisations due to the leakage of information by their employees. For example, a disgruntled employee may disclose proprietary information about his/her employers on a social networking site. Social networking is dichotomous in that an insider may use this platform to identify opportunities; however, the reverse is also possible in that the insider becomes an opportunity for a social engineer to exploit. Social engineering involves manipulating insiders to gain unauthorised access to a system or sensitive information [[36](#_ENREF_36)]. It appears that the more sophisticated an organisation becomes at perimeter protection, the more outsiders will turn to insiders to gain access. It is much easier for an outsider to exploit an insider than to try going through layers of protection [[37](#_ENREF_37)].

# 3. Related Work

A methodical review of technological tools available to minimise the insider threat may be found in Zeadally et al. [[38](#_ENREF_38)]. Mechanisms to undermine the insider threat include monitoring, detection, mitigation [[31](#_ENREF_31)] and deterrence. Data Loss Prevention (DLP) tools may be used to monitor data usage so as to detect and mitigate insider threats [[39](#_ENREF_39)]. Applying a DLP policy to control network services such as e-mail may deter potential insiders [[40](#_ENREF_40)]. DLP can assist for example to identify an insider that downloads classified documents and attaches it to an e-mail [[41](#_ENREF_41)]. Aside from system performance issues, a DLP may not be able to intercept a message that is encrypted [[41](#_ENREF_41)] or perhaps an insider who uses steganography to obfuscate an e-mail message [[42](#_ENREF_42)].

Currently the countermeasures that deter the abuse of internal systems focus on four factors, namely awareness of security policies, monitoring, preventive software and training [[43](#_ENREF_43)]. Monitoring alone is not sufficient for managing the insider threat, as it captures the intent but not the motivation. It is also difficult to identify patterns of misuse [[5](#_ENREF_5)]. Deterrents mechanisms cannot provide insight into the actual act of insider threat [[20](#_ENREF_20)]. From an information system security context, ‘deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures’ [[44](#_ENREF_44)]. General Deterrence theory has its roots in Rational Choice theory. It is moderated by certainty of detection, severity of punishment and the celerity of detection [[45](#_ENREF_45)]. Hence it focuses more on the costs of the crime, while Rational Choice theory considers both the costs and the benefits of the crime [[46](#_ENREF_46)]. Typically organisations rely on anti-virus systems and password protection schemes [[47](#_ENREF_47)] as deterrents. Antiviruses are only effective if they are updated consistently – which is a challenge, given the proliferation of new viruses. Authentication mechanisms do not effectively increase the effort involved in committing maleficence. Choi and Zage [[48](#_ENREF_48)] recommend that the location of an insider be used as an attribute for authentication so as to circumvent the insider threat. A robust authentication scheme could consist of a four factor scheme (i.e. ‘what you know’ (e.g. a password), ‘what you have’ (e.g. a smart card), or ‘what you are’ (e.g. a fingerprint) or ‘where you are’ (location)) [[48](#_ENREF_48)]. It is reasonable to assume that a four-factor authentication scheme is more resilient than a one-factor scheme (i.e. a typical password) authentication.

Several researchers have advocated profiling to predict future threats. An accurate profile of the insider may help to identify threats both prospectively and retrospectively [[49](#_ENREF_49)]. However, as Hunker and Probst [[5](#_ENREF_5)] claim, profiling has its drawbacks as it assumes that human behaviour is predictable. According to Brown et al. [[50](#_ENREF_50)] insiders cannot conceal their intentions over a long period of time. They suggest that an automated linguistic analyser be employed to correlate words with psychosocial factors in order to detect the insider threat.

Although intrusion detection systems are deployed to manage the insider threat, these systems have typically been designed for the external rather than the insider threat. Bowen et al. [[31](#_ENREF_31)] argue that intrusion detection mechanisms present a number of challenges ranging from false positives to difficulty in correctly identifying anomalous behaviour. Zeadally et al. [[38](#_ENREF_38)] remark that intrusion detection systems may be ineffective if an insider leaves no traces behind, because he/she has knowledge of how to disable the intrusion detection system. Schultz [[4](#_ENREF_4)] recommends the following indicators to detect the insider threat: personality traits, deliberate markers; preparatory behaviour; correlated usage patterns; verbal behaviour and meaningful errors. Some of these indicators may not be the most tangible sources of information; however, the elements relating to preparation may be. An insider has to prepare for an attack by searching for information and in doing so may make mistakes. A pattern to this preparation may be detected, such as issuing the same commands across all systems.

Unlike intrusion detection systems, honeypots do not suffer from false positives, as any interaction with a honeypot is bound to be illicit [[51](#_ENREF_51)]. A number of studies have been conducted on using honeypots to detect and identify the insider threat (see [[31](#_ENREF_31)] and [[52](#_ENREF_52)]). For example, McGrew et al. [[52](#_ENREF_52)] found that honeypots succeed in ‘sandboxing’ (i.e. containing) activities related to an insider threat. However, according to Spitzner [[51](#_ENREF_51)], honeypots have several disadvantages. There is a risk that an attacker may use a honeypot to harm other systems. Honeypots are only of value when an attacker interacts with them and they manage to capture actions related to this activity. In a way, the deployment of honeypots is an opportunity-based technique, as they provide an opportunity for an insider to commit maleficence.

Given the shortcomings associated with each technique, some researchers have considered an integrated approach. Brdiczka et al. [[53](#_ENREF_53)] used profiling and anomaly detection to detect the insider threat. Salem and Stolfo [[30](#_ENREF_30)] combined profiling and honeypots to reduce false positives. It is clear that managing the insider threat requires a wide-ranging approach and that no technique of its own accord is satisfactory. Some studies considered the opportunity dimension to create insider threat prediction tools (see [[54](#_ENREF_54)] and [[55](#_ENREF_55)]) in addition to attributes such as capability and motive. Theoharidou et al. [[10](#_ENREF_10)] conducted an examination on ISO17799 (a standard for information security at the time) and its relationship to managing the insider threat. The authors considered several criminology theories that could be used to enhance the standard. They found that crime theories like Situational Crime Prevention were not contemplated in the standard as they did not consider the opportunity side of crime. This omission in the previous and current standard is an indication that the notion of opportunity requires further exploration. This is further supported by Willison and Backhouse [[56](#_ENREF_56)]. They argue that a formal definition of opportunity within the cybercrime domain is lacking.

# 4. Understanding The Insider Threat From An Opportunity Theory Perspective

When considering the insider threat as a crime of opportunity, it is practical to reflect on the ten principles of opportunity theory as proposed by Felson and Clarke [[11](#_ENREF_11)]. This may lead to a better understanding of the insider threat and pave the way for the development of effective information security controls. Each of the subsequent subsections corresponds with a principle from Felson and Clarke [[11](#_ENREF_11)]. In a previous publication attention was drawn to the relationship between Felson and Clarke’s [[11](#_ENREF_11)] principles and the insider threat by [Padayachee [57]](#_ENREF_57). For the sake of completeness, this analogy is briefly described next however for a fuller discussion refer to [Padayachee [57]](#_ENREF_57)

## 4.1 Opportunity plays a role in causing all crime

This statement implies that an insider has to be given the opportunity to commit an offense.

## 4.2 Crime opportunities are highly specific

Reducing crime opportunities for insiders will have little impact on the outsider; hence strategies should be different for each type of attacker [[11](#_ENREF_11)]. As outsiders and insiders use different paths or approaches to attack systems [[58](#_ENREF_58)].

## 4.3 Crime opportunities are concentrated in time and space

According to Crime Pattern theory, crime opportunities are not equitably distributed in time and space, in other words, they are ‘clustered’ [[14](#_ENREF_14)]. For example, an insider may prefer to commit an offense after office/business hours when the transgression is assumed to be less conspicuous.

## 4.4 Crime opportunities depend on everyday movements of activity

According to Crime Pattern theory, offenders follow a spatial-temporal movement pattern in their daily life [[14](#_ENREF_14)]. Criminals are likely to commit initial crimes near these learned paths or activity nodes. It is possible to apply this concept to the activities that the insider performs online and to formulate virtual activity nodes. These activity nodes could consist of social networking sites, online recreational activities, the organisation’s intranet and search engines. Understanding the ‘nodes’ or activity spaces along which an insider operates in the virtual context may be key to discovering insider maleficence.

## 4.5 One crime produces opportunities for another

Felson and Clarke [[11](#_ENREF_11)] indicate that a major crime can result in other smaller crimes being committed and vice versa. Consequently, a single act of insider maleficence may be the key to discovering further acts of maleficence and serve to provide timely interventions.

## 4.6 Some products offer more tempting crime opportunities

The properties of Value, Inertia, Visibility, Accessibility (VIVA), based on Routine Activities theory, provide a point of reference for evaluating objects that are suitable targets [[13](#_ENREF_13)]. Objects that have high value, low inertia and high visibility, and that are easily accessible are more attractive to criminals [[11](#_ENREF_11)]. In a typical crime scenario, low inertia implies that an object is not easily transportable [[11](#_ENREF_11)]. In the cyber space context, Yar [[25](#_ENREF_25)] suggests that inertia may be related to the volume of data and the frustration caused by downloading large volumes of data.

## 4.7 Social and technological changes produce new crime opportunities

Felson and Clarke [[11](#_ENREF_11)] assert that a consumer product at the innovation stage is not attractive to criminals as it is still difficult to use. A product in the growth stage is more appealing as the product is more user-friendly. In the mass marketing stage, the demand for it increases. At saturation stage, the product is again not very attractive, because the demand for the product is now low. Reducing the life cycle to the core, it is clear that innovation would be highly valued by an insider threat.

## 4.8 Opportunities for crime can be reduced

Whereas Rational Choice, Routine Activities and Crime Pattern theories consider opportunity as a factor, Situational Crime Prevention theory is the most evolved theory with respect to opportunity-reducing techniques. Hence, this theory will be explored in more detail in Section 5 and will be used a basis for the thematic framework. Situational Crime Prevention theory considers five categories of opportunity-reducing measures. Each measure is further divided into 25 specific techniques [[9](#_ENREF_9)] which are intended for the physical landscape (see Table 1)

These techniques were given ‘digital analogies’ by Beebe and Roa [[23](#_ENREF_23)], Willison [[20](#_ENREF_20)], [Coles-Kemp and Theoharidou [22]](#_ENREF_22) and Hinduja and Kooi [[59](#_ENREF_59)]. The ‘increase the effort’ category involves ensuring criminal opportunities are difficult to execute which may discourage offenders, while the ‘increase the risks’ category involves increasing ‘the risk of detection, resistance and apprehension’ associated with maleficence [[60](#_ENREF_60)]. The ‘reduce the rewards’ category’ involves reducing the benefits of the crime [[60](#_ENREF_60)]. Beebe and Roa [[23](#_ENREF_23)] argue that lowering the perceived net benefit gained by cyber criminals may deter them from committing the crime. Nonetheless, in their opinion typical deterrents like sanctions are inadequate. They believe that the answer may lie in considering deterrents that do not only magnify the perceived effort required and inflate the perceived risk of being caught, but also decrease anticipated rewards.

‘Remove excuses’ involves neutralising the rationalisations of a criminal. [[60](#_ENREF_60)] The aforementioned category is significant for opportunity reduction because ‘if offenders can be prevented from rationalising and excusing their criminal actions, they will be open to feelings of guilt and shame’ [[20](#_ENREF_20)]. If an insider is unable to excuse and justify an offence, then the offence is not considered to be a suitable opportunity [[24](#_ENREF_24)]. For instance, insiders may rationalise their actions by perceiving cybercrime as a victimless crime [[61](#_ENREF_61)].

The ‘reduce provocations’ category involves removing ‘noxious stimuli from the environment’ [[60](#_ENREF_60)] that may precipitate a crime. This category considers the emotional side of crime which involves situations that act as triggers or precipitators to an individual who is already motivated [[9](#_ENREF_9)]. Examples of situations that precipitate maladaptive behaviour include frustrations caused by failures of equipment and services, and invasion of privacy [[62](#_ENREF_62)]. Wortley [[63](#_ENREF_63)] indicates that precipitator controls constitute more of a ‘soft’ approach, compared to the ‘hard’ approach of the previously discussed categories. Highly constrictive controls can lead to stress and frustration and hence precipitate crime. Hence, it is important for organisations to balance precipitator controls with cost-benefit controls.

Table 1

Techniques Of Situational Crime Prevention

|  |  |
| --- | --- |
| Category | Subcategories |
| Increase  the effort | Target hardening (i.e. increasing the difficulty of carrying out the crime [[60](#_ENREF_60)]); control of access to facilities; screen exits; deflecting offenders; controlling tools (i.e. tools that may be used to cause harm [[22](#_ENREF_22)]) |
| Increase  the risks | Extending guardianship; assisting natural surveillance; reducing anonymity; utilising place managers; strengthening formal surveillance |
| Reduce  the rewards | Concealing targets; removing targets; identifying property; disrupting markets; denying benefits |
| Reduce  provocations | Reducing frustrations and stress; avoiding disputes; reducing emotional arousal; neutralising peer pressure; discouraging imitation |
| Remove excuses | Setting rules; posting instructions; alerting conscience assisting compliance; controlling drugs and alcohol (this subcategory will not be considered in this study as it is unrelated to the information system domain) |

## 4.9 Reducing opportunities does not usually displace crime

Desistance implies either an end to all maleficence activity or displacement (i.e. deciding to commit another type of crime) [[12](#_ENREF_12)]. It is crucial to recognise that a prevention or deterrent strategy may result merely in maleficence being displaced by another type of cybercrime.

## 4.10 Focused opportunity reduction can produce wider declines in crime

A crime prevention method may provide the added benefit of diffusion [[11](#_ENREF_11)]. There is a hypothesis that an individual who is deterred from committing a crime in one circumstance assumes that the deterrence mechanism applies to other circumstances as well. This phenomenon is known as the diffusion of benefits [[11](#_ENREF_11)]. Such benefit may be derived when an insider assumes that the deterrent or prevention controls in one component of a system may be applicable to other components as well.

In the next section, contemporary information security techniques recommended for reducing opportunity from the perspective of Situational Crime Prevention theory are mapped to a contemporary set of best practices.

# 5. A Mapping Of Opportunity-Reducing Techniques In Information Security Against Best Practices

Willison [[20](#_ENREF_20)], as well as Coles-Kemp and Theoharidou [[22](#_ENREF_22)] mapped the ISO/IEC 27002 standard [[64](#_ENREF_64)] to Situational Crime Prevention theory (see Section 4.8). In the next elaboration, the current techniques recommend for Situational Crime Prevention is benchmarked against 19 best practices identified by Silowash et al. [[65](#_ENREF_65)]. As these best practices were developed from an analysis of more than 700 real world case studies (see Table 2), it is clear that this evaluation is based on the most definitive list of best practices recommended to mitigate the insider threat to date.

Table 2

Best Practices for Insider Threat Management [[65](#_ENREF_65)]

|  |  |
| --- | --- |
| 19 Best Practices for Insider Threat Management | |
|  | Consider threats from insiders and business partners in enterprise-wide risk. |
|  | Clearly document and consistently enforce policies and controls. |
|  | Incorporate insider threat awareness into periodic security training for all employees. |
|  | Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour. |
|  | Anticipate and manage negative issues in the work environment. |
|  | Know your assets. |
|  | Implement strict password and account management policies and practices. |
|  | Enforce separation of duties and least privilege. |
|  | Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities. |
|  | Institute stringent access controls and monitoring policies on privileged users. |
|  | Institutionalize system change controls. |
|  | Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions. |
|  | Monitor and control remote access from all end points, including mobile. |
|  | Develop a comprehensive employee termination procedure. |
|  | Implement secure backup and recovery processes. |
|  | Develop a formalized insider threat program. |
|  | Establish a baseline of normal network behaviour. |
|  | Be especially vigilant regarding social media. |
|  | Close the doors to unauthorized data exfiltration. |

Guido and Brooks [[40](#_ENREF_40)] also established a set of practices based on a systematic review of known insider threat best practices. The practices offered by Guido and Brooks [[40](#_ENREF_40)] are considered in instances where best practices listed in Table 2 is deficient. This benchmarking process superimposes these best practices on Situational Crime Prevention in order to derive a pragmatic framework to mitigate the insider threat (see Appendix A).

## 5.1 Increase the effort

The ‘increase the effort’ category describes interventions that increase the difficulty associated with maleficence. Table 3 summarises the techniques and the accompanying best practices.

Table 3

Increase the effort mapping

|  |  |  |
| --- | --- | --- |
| Subcategory | Proposed Techniques | Best Practice Mapping |
| Target  hardening | Anti-virus software [[20](#_ENREF_20)];vulnerability patching [[23](#_ENREF_23)]; sensitive system isolation [[22](#_ENREF_22)]; extraneous ports closed[[59](#_ENREF_59)]; custom installs[[59](#_ENREF_59)];proper password policies [[59](#_ENREF_59)] | **#7** Implement strict password and account management policies and practices |
| Control access to facilities | Authentication [[22](#_ENREF_22)] | **# 10** Institute stringent access controls and monitoring policies on privileged |
| Screen exits | Firewalls[[20](#_ENREF_20)]; ingress/egress filtering[[59](#_ENREF_59)]; internet protocol (IP)-based restrictions [[59](#_ENREF_59)] | **# 19** Close the doors to unauthorized data exfiltration |
| Deflecting offenders | Honeypots [[23](#_ENREF_23)]; key splitting [[22](#_ENREF_22)]; segregation of duties [[20](#_ENREF_20)]; background checks on employees (i.e. pre-screening [[20](#_ENREF_20)]); offsite storage of data[[59](#_ENREF_59)] | **#4** Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.  **#8** Enforce separation of duties and least privilege |
| Controlling tools | Web access controls [[22](#_ENREF_22)]; filter of downloads of illicit tools (i.e. controlling downloads [[20](#_ENREF_20)]);termination procedures [[20](#_ENREF_20)]; principle of least privilege [[22](#_ENREF_22)]; file access permission [[59](#_ENREF_59)]. | **#8** Enforce separation of duties and least privilege.  **#14** Develop a comprehensive employee termination procedure. |

The information security analogy proposed for ‘target hardening’(i.e. increasing the difficulty of carrying out the crime [[60](#_ENREF_60)]) include anti-virus software [[20](#_ENREF_20)], vulnerability patching [[23](#_ENREF_23)] and ‘sensitive system isolation’ [[22](#_ENREF_22)]. Antiviruses are susceptible to misuse. Vulnerability patches may be exploited if organisations do not apply the patches immediately [[66](#_ENREF_66)]. ‘Sensitive system isolation’ may be more susceptible to insider threats, as storing all the sensitive and confidential data in one location makes it an easy target [[37](#_ENREF_37)] which defeats the purpose of ‘target hardening’. In this subcategory it was established that Practice #7 (i.e. ‘Implement strict password and account management policies and practices’) parallels the essence of this subcategory.

Authentication [[22](#_ENREF_22)] has been proposed to ‘control access to facilities’. However, as described in Section 3, a four-factor authentication scheme will be more resilient than a lower order factor authentication. Traditional access control such as role-based control is also susceptible to the insider threat as the system grants access as long as the access is authorised [[67](#_ENREF_67)]. Usage control may be more effective, since it considers the missing components of traditional access control − that is obligations and conditions [[68](#_ENREF_68)]. Hence, finer-grained authentication and access control may be an effective means of addressing the technique of ‘control access to facilities’. It is evident that practice #10 (i.e. ‘Institute stringent access controls and monitoring policies on privileged’) is most appropriate to this subcategory.

Firewalls, which have been proposed as a digital analogy to ‘screen exits’ [[20](#_ENREF_20)] are ‘of limited use, given that the majority of insider threat activity occurs within an enterprise’s perimeter’ [[40](#_ENREF_40)]. Clearly this subcategory parallels practice #19 (i.e. ‘Close the doors to unauthorized data exfiltration’).

The information security controls proposed for ‘deflecting offenders’ include: honeypots [[23](#_ENREF_23)]; key splitting [[22](#_ENREF_22)]; ‘segregation of duties’ [[20](#_ENREF_20)] and pre-screening [[20](#_ENREF_20)]. ‘Segregation of duties’ prevents misuse since duties and responsibilities are separated [[64](#_ENREF_64)]. The techniques in this subcategory parallel practices #4 (i.e. ‘Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour’) and #8 (i.e. ‘Enforce separation of duties and least privilege’).

Web access controls [[22](#_ENREF_22)], ‘controlling downloads’ [[20](#_ENREF_20)], ‘termination procedures’ [[20](#_ENREF_20)] and ‘least privilege’ [[22](#_ENREF_22)]) have been proposed as information security measures with respect to ‘controlling tools’ ( i.e. tools that may be used to cause harm). The filtering of downloads is an essential control as insiders may download illicit tools like keystroke loggers or stenographers [[69](#_ENREF_69)] to aid them in committing maleficence. The principle of ‘least privilege’ is another fundamental control however; its practical enforcement may be limited due to fluctuations in work responsibilities. It is clear that this subcategory can be superimposed to practices #8 (i.e. ‘Enforce separation of duties and least privilege’) and practice #14 (i.e. ‘Develop a comprehensive employee termination procedure’). It is proposed that ‘filtering of downloads’ is an essential control hence this should also be considered as a best practice.

## 5.2 Increase the risks

This category proposes interventions that increase the negative consequences associated with maleficence. Table 4 summarises the techniques and the accompanying best practices.

The information security control that are suggested for ‘extending guardianship’ involves the management of mobile facilities [[20](#_ENREF_20)]. This is significant as the privacy offered by remote access ‘provides a tempting opportunity for insiders to attack with less risk’ [[27](#_ENREF_27)]. This correlates with best practice #13 (i.e. ‘Monitor and control remote access from all end points, including mobile’)

Table 4

Increase the risks mapping

|  |  |  |
| --- | --- | --- |
| Subcategory | Recommended techniques | Best Practice Mapping |
| *Extending guardianship* | Mobile computing and teleworking [[64](#_ENREF_64)] | **#13** Monitor and control remote access from all end points, including mobile |
| *Assisting natural*  *surveillance* | Incident reporting [[22](#_ENREF_22)]; visualisation tools [[23](#_ENREF_23)]. | **#16** Develop a formalized insider threat program (includes an insider response plan.) |
| *Reducing anonymity* | Audit trails and event logging [[20](#_ENREF_20)]. | **#12** Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions. |
| *Utilising place*  *managers* | Two-person sign-off [[20](#_ENREF_20)]; | No Equivalent Practice |
| *Strengthening formal*  *surveillance* | Intrusion detection [[20](#_ENREF_20)]; resource usage monitoring [[23](#_ENREF_23)] | **#11** Institutionalize system change controls.  **#17** Establish a baseline of normal network behaviour. |

The information security controls that are recommended for ‘assisting natural surveillance’ include incident reporting [[22](#_ENREF_22)] and visualisation tools [[23](#_ENREF_23)]. Cappelli et al. [[27](#_ENREF_27)] further qualify this process by affirming that there should be a specific Insider Incident Response Plan. This correlates with practice #16 (i.e. ‘Develop a formalized insider threat program’) which includes incident management. Silowash et al. [[65](#_ENREF_65)] asserts that an insider threat programme should include ‘an established incident response plan that addresses incidents perpetrated by insiders, has an escalation chain, and delineates authorities for deciding disposition.’

The information security controls that are recommended to facilitate ‘reducing anonymity’ include audit trails and event logging [[20](#_ENREF_20)].This relates to practice #12 (i.e. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions’).

The information security techniques proposed for ‘utilising place managers’ include a two-person sign-off [[70](#_ENREF_70)] and ‘resource usage monitoring’ [[71](#_ENREF_71)]. A two-person sign-off will help “reduce the risk of extortion” [[72](#_ENREF_72)]. Two-person controls mirror the thematic concept of multiparty control. Multiparty control is more suitable to ‘utilising place managers’ technique, as it involves employees who could naturally monitor the environment as a deterrent [[73](#_ENREF_73)] while ‘monitoring resource usage’ may be more suitable to ‘strengthening formal surveillance’ technique. Multiparty controls was not considered a best practice by either Silowash et al. [[65](#_ENREF_65)] nor Guido and Brooks [[40](#_ENREF_40)].

Intrusion detection is recommended as a control for ‘strengthening formal surveillance’[[20](#_ENREF_20)]. Intrusion detection systems may not be sensitised to the commands issued by a malicious insider and may appear to be part of his/her normal duties [[74](#_ENREF_74)]. Hence practice #17 (i.e. ‘Establish a baseline of normal network behavior’) may assist in developing more effective intrusion detection systems and resource usage monitoring. Formal surveillance can be strengthened by change controls and configuration management tools where the former ensure the proper management of all changes made to the network and the latter detect changes to source code and application files [[27](#_ENREF_27)]. This addition correlates with practice #11 (i.e. ‘Institutionalize system change controls’.)

## 5.3 Reduce the rewards

The ‘reduce the rewards’ category is accomplished by decreasing the perceived benefits associated with committing crime. Table 5 summarises the techniques and the accompanying best practices.

Table 5

Reduce The Rewards Mapping

|  |  |  |
| --- | --- | --- |
| Subcategory | Recommended  Techniques | Best Practice Mapping |
| *Concealing targets* | Low public profile regarding the location of secure systems [[59](#_ENREF_59)]) | No Equivalent Practice |
| *Removing targets* | Clear desk and clear screen [[64](#_ENREF_64)]; | No Equivalent Practice |
| *Identifying property* | Watermarking [[23](#_ENREF_23)]; digital signatures [[20](#_ENREF_20)]; information classification [[23](#_ENREF_23)]; | **#6** Know your assets. |
| *Denying*  *benefits* | Encryption [[20](#_ENREF_20)]; automatic data destruction mechanisms [[23](#_ENREF_23)];continuity management [[22](#_ENREF_22)]; incident management [[22](#_ENREF_22)] | **#15** Implement secure backup and recovery processes. |
| *Disrupting markets* | Open source products or freeware | No Equivalent Practice |

The information security analogy for ‘concealing targets’ involves restricting public domain information, for example constraining the information that is revealed on the organisation’s website [[20](#_ENREF_20)]. This is an essential control, as social engineers may exploit information provided on an organisation’s website, while insiders may use the organisation’s intranet to identify opportunities. However there is no equivalent best practice for this subcategory. ‘Removing targets’ is a related technique that involves the obscuring of targets by deploying Clear Desk and Clear Screen controls as recommended by the ISO/IEC 27002 standard [[64](#_ENREF_64)]. No equivalent best practice could be linked to this subcategory. Clearly there is need to develop best practices for these two subcategories.

Watermarking [[23](#_ENREF_23)], digital signatures [[20](#_ENREF_20)] and ‘information classification’ [[23](#_ENREF_23)] have been recommended as information security analogies for ‘identifying property’. Watermarking is rendered ineffective if the insider has access to the original object [[75](#_ENREF_75)]. Digital signatures may prove useful for non-repudiation; however, they require additional validation such as time stamps [[76](#_ENREF_76)]. Asset management (ISO/IEC 27002) is more encompassing than mere ‘information classification’ as it includes accountability for assets [[64](#_ENREF_64)]. Hence a fitting best practice would be practice #6 (i.e. ‘Know your assets’).

Encryption [[20](#_ENREF_20)], Automatic Data destruction Mechanisms [[23](#_ENREF_23)],Continuity Management [[22](#_ENREF_22)] and Incident Management [[22](#_ENREF_22)] are offered as information security techniques analogous to the ‘denying benefits’ technique. Encryption may be cracked by insiders using keystroke loggers [[27](#_ENREF_27)] or by the mere fact that insiders have privileged access [[26](#_ENREF_26)]. The automatic destruction of data by mechanisms that wipe out sensitive data instantly reduces the suitability of a target [[19](#_ENREF_19)]. Business Continuity Management and Information Security Incident Management are clauses from ISO/IEC 27002 [[77](#_ENREF_77)]. Manage Continuity also implies Disaster Recovery [[77](#_ENREF_77)]. This correlates with best practice # 15 (i.e. ‘Implement secure backup and recovery processes’).

With regard to the ‘disrupting markets’ technique, open source products or freeware are recommended as information security controls. This may not be financially viable. There is no corresponding practice that could be linked to this subcategory.

## 5.4 Reduce provocations

The ‘reduce provocations’ category consists of techniques that are aimed at decreasing the emotional triggers that may precipitate a motivated criminal to commit an offence. This paper proposes a more coherent term to designate the ‘reduce provocations’ category namely ‘reduce precipitators’ in order to focus on the situational factors rather than purely on the emotional side of crime. The purpose of this new designation is to reflect the pluralistic nature of cybercrime interventions (i.e. technological, psychological, sociological and organisational). Adaptions of this nature are congruent with the principles of Situational Crime Prevention. Cornish and Clarke [[9](#_ENREF_9)] posit that the application of Situational Crime Prevention theory must be predicated on the crime itself. As each crime is unique, the opportunity-reducing measures must also differ. Table 6 summarises the techniques and the accompanying best practices

Some of the proposed analogies are more generic than specific to the cyber security domain. For the emotional side such as ‘reducing frustrations and stress’, ‘avoiding disputes’, ‘reducing emotional arousal’ can be mitigated by practice #5 (i.e. ‘Anticipate and manage negative issues in the work environment’) which is an overarching practice.

The technique of ‘discouraging imitation’ may be resolved by ‘rapid repair’ of damage inflicted on an organisation’s information technology (IT) infrastructure, for example the prompt repair of a defaced website [[20](#_ENREF_20)]. This can be correlated with practice # 15 (i.e. ‘Implement secure backup and recovery processes’).

Coles-Kemp and Theoharidou [[22](#_ENREF_22)] recommend security usability and user participation in the risk analysis process as possible information security controls for ‘reducing emotional arousal’. User participation in general would be beneficial, as the insider threat may be precipitated by security policies or controls that are misunderstood, poorly communicated or inconsistently applied [[65](#_ENREF_65)], as well as by a lack of procedural fairness [[78](#_ENREF_78)]. Hence, it may be useful to involve users in the entire information security life cycle from development to implementation. Security usability could be a step towards reducing the insider’s negative response towards information security controls. Users should be able to figure out how to perform security tasks and they should be comfortable with the user interface [[79](#_ENREF_79)]. As discussed earlier this was correlated with practice #5 (i.e. ‘Anticipate and manage negative issues in the work environment’).

Disciplinary processes [[22](#_ENREF_22)] have been recommended as a means of ‘neutralising peer pressure’. This may not be apt to this category – controls that identify elements of peer pressure would be more suitable. Social engineering is a virtual form of peer pressure. An insider may act as a social engineer and implement techniques like desk snooping or shoulder surfing to gather evidence with which to manipulate another insider as a means of identifying opportunities [[69](#_ENREF_69)]. Hence, it is recommended that this technique be expanded so as to neutralise the effect of social engineers. This parallels practice #18 (i.e. ‘Be especially vigilant regarding social media’). Practice #18 should also include a clause about social engineers. While Practice # 1 (i.e. ‘Consider threats from insiders and business partners in enterprise-wide risk’) is also important, as an insider may be influenced by ‘outsiders’ to commit maleficence.

Table 6

Reduce Precipitators Mapping

|  |  |  |
| --- | --- | --- |
| Subcategory | Recommended  Techniques | Best Practice Mapping |
| *Reducing frustrations and stress* | Supportive working environment [[22](#_ENREF_22)]; support whistle-blowers [[20](#_ENREF_20)]. | **#5** Anticipate and manage negative issues in the work environment. |
| *Avoiding disputes* | Dispute resolution | **#5** Anticipate and manage negative issues in the work environment |
| *Reducing emotional arousal* | Security usability[[22](#_ENREF_22)]; user participation in the risk analysis process[[22](#_ENREF_22)] | **#5** Anticipate and manage negative issues in the work environment |
| *Neutralising peer pressure* | Disciplinary processes [[22](#_ENREF_22)] | **#1** Consider threats from insiders and business partners in enterprise-wide risk  **#18** Be especially vigilant regarding social media |
| *Discouraging imitation* | Prompt repair (i.e. of damage inflicted on an organization’s information technology (IT) infrastructure [[20](#_ENREF_20)]) | **#15** Implement secure backup and recovery processes |

## 5.5 Remove excuses

The ‘remove excuses’ category is accomplished by interventions that decrease the rationalisations that criminals may use to justify their behaviour. Table 7 summarises the techniques and the accompanying best practices.

In terms of ‘setting rules’, the techniques parallel practices # 2 (i.e. ‘Clearly document and consistently enforce policies and controls’) and #9 (i.e. ‘Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities’).

In terms of ‘posting instructions’, e-mail disclaimers [[23](#_ENREF_23)] are recommended as a comparable information security control, aside from the typical controls like information security policy. There is no equivalent practice found in the set of benchmark practices. However the best practice of ‘Issue rules of behaviour to all users and implement banners on all systems’ proposed by Guido and Brooks [[40](#_ENREF_40)]is appropriate to this subcategory.

Single sign-on [[20](#_ENREF_20)] and ‘a single point of reference for security’ [[22](#_ENREF_22)] have been proposed as information security controls to realise the ‘assisting compliance’ technique. Single sign-on is a process where an insider is given one password across all systems, which assists with usability and may be centrally controlled [[80](#_ENREF_80)]. According to Kelly [[81](#_ENREF_81)], having a single password has several advantages: users are unlikely to write it down or to constantly call the helpdesk to assist with the resetting of passwords. These advantages reduce the exposure of the insider to social engineering attacks. Single sign-on is considered to be an aspect of Centralised User Management [[82](#_ENREF_82)]. This notion extends to the ‘single point of reference for security’ technique, which involves the centralised management of information security policies. Hence, ‘Centralise Insider Threat Management’ should be proposed as a best practice for ‘assisting compliance’. While best practice #3 (i.e. ‘Incorporate insider threat awareness into periodic security training for all employees’) is absolutely essential in assisting compliance.

Table 7

Remove excuses mapping

|  |  |  |
| --- | --- | --- |
| Subcategory | Recommended  Techniques | Best Practice Mapping |
| *Setting rules* | Policies, agreements, procedures such as acceptable use policy [[59](#_ENREF_59)]; employee assistance programme [[59](#_ENREF_59)] | **#2** Clearly document and consistently enforce policies and controls  **#9** Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities. |
| *Posting instructions* | E-mail disclaimers [[23](#_ENREF_23)] | Issue rules of behaviour to all users and implement banners on all systems. |
| *Assisting compliance* | Single sign-on [[20](#_ENREF_20)]; ethically sound business practices [[59](#_ENREF_59)]; single point of reference for security [[22](#_ENREF_22)]; promotion of a healthy work environment [[59](#_ENREF_59)] | **#3** Incorporate insider threat awareness into periodic security training for all employees. |
| *Alerting conscience* | Copyright protection [[22](#_ENREF_22)]; code of ethics [[22](#_ENREF_22)]; warning messages when logging in[[59](#_ENREF_59)];. multi-level warning banners [[23](#_ENREF_23)] | Issue rules of behaviour to all users and implement banners on all systems. |

In terms of ‘alerting conscience’, the information security controls that are recommended include copyright protection [[22](#_ENREF_22)]; a code of ethics [[22](#_ENREF_22)] and ‘multi-level warning banners’ [[23](#_ENREF_23)]. Copyright protection is addressed by the ‘setting rules’ category. Practice #3 (Incorporate insider threat awareness into periodic security training for all employees) would be an adequate way to alert conscience. However Guido and Brooks [[40](#_ENREF_40)] best practice recommendation of ‘Issue rules of behaviour to all users and implement banners on all systems’ is more appropriate in this case.

Fig. 1. A Summary of percentage correlations of best practices per category.

A summary of the correlation of the practices per category is shown in fig 1. The cost-benefit type categories such as ‘increase the effort’, ‘increase the risk’ and ‘reduce the reward’ challenges the rational insider to calculate the net value of the crime. The ‘remove excuses’ and ‘reduce precipitators ‘categories, on the other hand, are indirect controls that force an insider to consider a crime opportunity from a rational perspective without being driven by provocations or justifications. It is clear that the best practices focus more on the costs of cybercrime rather than the reducing the benefits of cybercrime.

# 6. discussion of findings

In this evaluation, it was found that all 19 best practices derived from empirical research were satisfied by Situational Crime Prevention. This implies that Situational Crime Prevention is highly compliant with best practices. This implies that implementing Situational Crime Prevention is an example of best practice. However the application of Situational Crime Prevention will require considering these best practices from an opportunity-reducing lens.

Some best practices were overarching and fitted more than one subcategory. Notably six of the 24 subcategories could not be linked with the best practices from Silowash et al. [[65](#_ENREF_65)]. While two of these subcategories were satisfied by one of the best practices proposed by Guido and Brooks[[40](#_ENREF_40)]. However, four techniques were incomparable to a best practice. To be precise, 16.67% techniques were incomparable to a best practice. This clearly highlights the gaps where insider threat programs are lacking. The category of ‘reduce the rewards’ category were found to be the most incongruent to best practices – specifically the sub-categories of ‘concealing targets’, ‘removing targets’ and ‘disrupting markets’. The author provided recommendations in instances where there were no analogous best practices (see Appendix 1).

In a similar study, Beebe and Roa [[71](#_ENREF_71)] claim that the majority of security interventions are introduced to increase the perceived effort, while, limited controls increase the perceived risk and reduce the anticipated rewards. Their study enumerated the number of techniques per category. In the current study, it was found that the majority of best practices are aimed at increasing the effort and the increasing the risk of cybercrime while the least number of practices are aimed at reducing the rewards of cybercrime. Removing the excuses (i.e. justifications) for maleficence is also found to be inadequate. In this evaluation it is clear the reducing the rewards associated with crime is a highly overlooked area with respect to best practices. This implies that even though the cost of crime is high, the rewards are still attractive.

# 7. CONCLUSION

This paper makes three significant contributions to the understanding and mitigating of insider threat. Firstly, the framework derived here may be used as a proactive mitigation strategy – it seeks to conceptualise the element of opportunity in terms of the insider threat. The framework may be used to implement information security controls that should empower information security administrators to prevent and possibly counteract the insider threat. Future research will involve evaluating the framework that was derived from opportunity-based criminology theories and best practices. Secondly, in the process of deriving the framework, several areas of potential research were revealed. The third contribution involves benchmarking best practices with respect to Situational Crime Prevention. This analysis has demonstrated the extensibility of the extant security best practices that could be enhanced with an opportunity-reducing dimension. The main contribution made by this article is the multidimensionality of the framework, which provides a new solution space in which to reason about mitigating insider threat from a best practices and an opportunity-reducing perspective.

# References

[1] CSO MAGAZINE, USSS, CERT, and Deloitte. (2011, 12 March 2013). *2011 Cybersecurity Watch Survey: Organizations need more skilled cyber professionals to stay secure*. Available: [www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf](http://www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf)

[2] IT Governance. (2013). *Boardroom Cyber Watch 2013: Report*. Available: [www.itgovernance.co.uk/what-is-cybersecurity/boardroom-cyber-watch.aspx](http://www.itgovernance.co.uk/what-is-cybersecurity/boardroom-cyber-watch.aspx)

[3] G. B. Magklaras and S. M. Furnell, “A preliminary model of end user sophistication for insider threat prediction in IT systems”, *Computers & Security,* Vol. 24, No. 5, 2005, pp. 371-380.

[4] E. E. Schultz, “A framework for understanding and predicting insider attacks”, *Computers & Security,* Vol. 21, No. 6, 2002, pp. 526-531.

[5] J. Hunker and C. W. Probst, “Insiders and insider threats-an overview of definitions and mitigation techniques”, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* Vol. 2, No. 1, 2011, pp. 4-27.

[6] R. Chinchani, A. Iyer, H. Q. Ngo, and S. Upadhyaya, "Towards a theory of insider threat assessment," in *International Conference on Dependable Systems and Networks*, Yokohama, Japan, 2005, pp. 108-117.

[7] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research: Beyond the hacker",*Insider Attack and Cyber Security*, Advances in Information Security S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, W. S. Smith, and S. Sinclair, eds., pp. 69-90, New York: Springer US, 2008.

[8] K. Nance and R. Marty, "Identifying and visualizing the malicious insider threat using bipartite graphs," in *44th Hawaii International Conference on System Sciences (HICSS)*, Koloa, Kauai, *Hawaii*, USA, 2011, pp. 1-9.

[9] D. B. Cornish and R. V. Clarke, “Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention”, *Crime Prevention Studies,* Vol. 16, 2003, pp. 41-96.

[10] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, “The insider threat to information systems and the effectiveness of ISO17799”, *Computers & Security,* Vol. 24, No. 6, 2005, pp. 472-484.

[11] M. Felson and R. V. Clarke, "Opportunity makes the thief: Practical theory for crime prevention," Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, London Police Research Series Paper 98, 1998.

[12] R. V. Clarke and D. B. Cornish, “Modeling offenders' decisions: A framework for research and policy”, *Crime and Justice,* Vol. 6, 1985, pp. 145-185.

[13] L. E. Cohen and M. Felson, “Social change and crime rate trends: A routine activity approach”, *American Sociological Review* Vol. 44, No. 4, 1979, pp. 588-608.

[14] P. Brantingham and P. Brantingham, "Crime Pattern Theory",*Environmental Criminology and Crime Analysis*, R. Wortley and L. Mazerolle, eds., pp. 78-93, New York: Macmillian, 2008.

[15] R. V. Clarke, "Introduction",*Situational Crime Prevention: Successful Case Studies*, R. V. Clarke, ed., pp. 1-43, Guilderland, NY: Harrow and Heston, 1997.

[16] G. S. Becker, “Crime and Punishment: An Economic Approach”, *Journal of Political Economy,* Vol. 76, No. 2, 1968, pp. 169-217.

[17] H. Li, J. Zhang, and R. Sarathy, “Understanding compliance with internet use policy from the perspective of rational choice theory”, *Decision Support Systems,* Vol. 48, No. 4, 2010, pp. 635-645.

[18] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness”, *MIS Quarterly,* Vol. 34, No. 3, 2010, pp. 523-548.

[19] P. H. Hartel, M. Junger, and R. J. Wieringa, "Cyber-crime Science = Crime Science + Information Security," Centre for Telematics and Information Technology University of Twente, Enschede TR-CTIT-10-34, 2010.

[20] R. Willison, “Understanding the perpetration of employee computer crime in the organisational context”, *Information and Organization,* Vol. 16, No. 4, 2006, pp. 304-324.

[21] R. Willison and M. Siponen, “Overcoming the insider: Reducing employee computer crime through situational crime prevention”, *Communications of the ACM,* Vol. 52, No. 9, 2009, pp. 133-137.

[22] L. Coles-Kemp and M. Theoharidou, "Insider threat and information security management",*Insider Threats in Cyber Security*, C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, eds., pp. 45-71, US: Springer, 2010.

[23] N. L. Beebe and V. S. Roa, "Using situational crime prevention theory to explain the effectiveness of information systems security," in *2005 SoftWars Conference*, Las Vegas, Nevada, 2005, pp. 1-18.

[24] N. L. Beebe and V. S. Roa, “Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process”, *Communications of the Association for Information Systems,* Vol. 26, No. 1, 2010, pp. 329-358.

[25] M. Yar, “The novelty of ‘cybercrime’an assessment in light of routine activity theory”, *European Journal of Criminology,* Vol. 2, No. 4, 2005, pp. 407-427.

[26] R. Walton, “Balancing the insider and outsider threat”, *Computer fraud & security,* Vol. 11, 2006, pp. 8-11.

[27] M. Cappelli, A. P. Moore, and T. J. Shimeall. (2006). *Common sense guide to prevention/detection of insider threats* Available: <http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.11070118.pdf> (Carnegie Mellon University, CyLab and the Internet Security Alliance, Tech. Rep.)

[28] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, “Insiders behaving badly: addressing bad actors and their actions”, *IEEE Transactions on Information Forensics and Security,* Vol. 5, No. 1, 2010, pp. 169-179.

[29] M. Bishop and C. Gates, "Defining the insider threat," in *4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*, Oak Ridge, Tennesse, USA, 2008, pp. 15:1-15:3.

[30] M. B. Salem and S. J. Stolfo, “Combining baiting and user search profiling techniques for masquerade detection”, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA),* Vol. 3, No. 1/2, 2012, pp. 13-29.

[31] B. M. Bowen, M. B. Salem, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, “Designing host and network sensors to mitigate the insider threat”, *IEEE Security & Privacy,* Vol. 7, No. 6, 2009, pp. 22-29.

[32] D. F. Anderson, D. Cappelli, J. J. Gonzalez, M. Mojtahedzadeh, A. Moore, R. Elliot*, et al.*, "Preliminary system dynamics maps of the insider cyber-threat problem," in *22nd International Conference of the System Dynamics Society*, Oxford, England, 2004, pp. 25-29.

[33] B. J. Wood, "An insider threat model for adversary simulation," presented at the Research on mitigating the Insider Threat to Information Systems Arlington, Virginia, 2000.

[34] W. R. Claycomb and A. Nicholl, "Insider threats to cloud computing: Directions for new research challenges," in *IEEE 36th Annual Computer Software and Applications Conference(COMPSAC)*, Izmir, Turkey, 2012, pp. 387-394.

[35] N. N. A. Molok, A. Ahmad, and S. Chang, "Understanding the factors of information leakage through online social networking to safeguard organizational information," presented at the 21st Australasian Conference on Information Systems, Brisbane, Australia, 2010.

[36] P. Damie. (2002, 21 September 2013). *Social Engineering: A Tip of the Iceberg*. Available: <http://www.isaca.org/Content/ContentGroups/Journal1/20023/Social_Engineering_A_Tip_of_the_Iceberg.htm>.

[37] A. Jones and C. Colwill, "Dealing with the malicious insider," in *6th Australian Information Security Management Conference*, Perth, 2008, pp. 87-100.

[38] S. Zeadally, Y. Byunggu, H. J. Dong, and L. Liang, “Detecting insider threats: Solutions and trends”, *Information Security Journal: A Global Perspective,* Vol. 21, No. 4, 2012, pp. 183-192.

[39] G. J. Silowash and C. King. (2013, 10 July 2013). *Insider threat control: Understanding data loss prevention (DLP) and detection by correlating events from multiple sources*. Available: <http://repository.cmu.edu/sei/708>

[40] M. D. Guido and M. W. Brooks, "Insider threat program best practices," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, 2013, pp. 1831-1839.

[41] A. Joch. (2011). *Why you can't stop insider threats: You can only hope to contain them*. Available: <http://fcw.com/articles/2011/02/28/feat-cybersecurity-insider-threats.aspx>

[42] E. Cole and S. Ring, *Insider threat: Protecting the enterprise from sabotage, spying, and theft*, first edition, chapter 2 ed. Rockland, Maine: Syngress, 2006.

[43] D. D'Arcy and A. Hovav, “Does one size fit all? Examining the differential effects of IS security countermeasures”, *Journal of Business Ethics,* Vol. 89, 2009, pp. 57-71.

[44] H. F. Tipton, "Types of information security controls",*Handbook of Information Security Management*, M. Krause and H. F. Tipton, eds., pp. 1357-1366, Boca Raton: CRC press, 2007.

[45] D. D'Arcy and T. Herath, “A review and analysis of deterrence theory in the IS security literature: making sense of disparate findings”, *European Journal of Information Systems,* Vol. 20, 2011, pp. 643-658.

[46] G. F. Vito, J. R. Maahs, and R. M. Holmes, *Criminology: Theory, Research, and Policy*, second edition, chapter 3 ed. Boston: Jones & Bartlett Learning, 2006.

[47] S. M. Lee, S. Lee, and S. Yoo, “An integrative model of computer abuse based on social control and general deterrence theories”, *Information and Management* Vol. 41, No. 6, 2003, pp. 707-718.

[48] S. Choi and D. Zage, "Addressing insider threat using “where you are” as fourth factor authentication," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, Boston, Massachusetts, 2012 pp. 147-153.

[49] N. Nykodym, R. Taylor, and J. Vilela, “Criminal profiling and insider cyber crime”, *Digital Investigation,* Vol. 2, No. 4, 2005, pp. 261-267.

[50] C. R. Brown, A. Watkins, and F. L. Greitzer, "Predicting insider threat risks through linguistic analysis of electronic communication," in *46th Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 2013, pp. 1849-1858.

[51] L. Spitzner, "Honeypots: Catching the insider threat," in *19th Annual Computer Security Applications Conference(ACSAC 2003)*, Las Vegas, USA, 2003, pp. 170-179.

[52] R. McGrew, B. Rayford, and J. R. Vaughn, "Experiences with honeypot systems: Development, deployment, and analysis," in *39th Annual Hawaii International Conference on System Sciences (HICSS’06)*, Maui, Hawaii, USA, 2006, pp. 220a-220a.

[53] O. Brdiczka, J. Liu, B. Price, J. Shen, A. Patil, R. Chow*, et al.*, "Proactive insider threat detection through graph learning and psychological context," in *IEEE Symposium on Security and Privacy Workshops (SPW)*, San Francisco, USA, 2012, pp. 142 -149.

[54] G. B. Magklaras and S. M. Furnell, “Insider threat prediction tool: Evaluating the probability of IT misuse”, *Computers & Security,* Vol. 21, No. 1, 2002, pp. 62-73.

[55] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An insider threat prediction model",*Trust, Privacy and Security in Digital Business*, Lecture Notes in Computer Science S. Katsikas, J. Lopez, and M. Soriano, eds., pp. 26-37, Berlin Heidelberg: Springer 2010.

[56] R. Willison and J. Backhouse, “Opportunities for computer crime: Considering system risk from a criminological perspective”, *European Journal of Information Systems,* Vol. 15, No. 4, 2006, pp. 403-414.

[57] K. Padayachee, "A Conceptual Opportunity-Based Framework To Mitigate The Insider Threat" in *Proceedings of the Information Security for South Africa (ISSA 2013)*, Johannesburg, South Africa, 2013, pp. 1-6.

[58] Y. Quassai and B. Panda, “Insider threat mitigation: preventing unauthorized knowledge acquisition”, *International Journal of Information Security,* Vol. 11, No. 4, 2012, pp. 269-280.

[59] S. Hinduja and B. Kooi, “Curtailing cyber and information security vulnerabilities through situational crime prevention”, *Security Journal,* Vol. 26, No. 4, 2013, pp. 383-402.

[60] T. R. Smith and J. Scott "Policing and Crime prevention",*Crime prevention*, D. A. Mackey and K. Levan, eds., pp. 61-88, Burlington, Massachusetts: Jones & Bartlett, 2011.

[61] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis. (2013, Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*. Available: <http://dx.doi.org/10.1016/j.cose.2013.05.006>.

[62] R. Wortley, “A classification of techniques for controlling situational precipators of crime”, *Security Journal,* Vol. 14, 2001, pp. 63-82.

[63] R. Wortley, “A two-stage model of situational crime prevention”, *Studies on Crime and Crime Prevention,* Vol. 7, 1998, pp. 173-188.

[64] ISO/IEC 27002:2005. (2005). *Information Technology—Security Techniques—Information Security Management Systems—Code of Practice for Information Security Management*. Available: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>

[65] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. Shimeall, and L. Flynn. (2012). *Common sense guide to mitigating Insider threats*. Available: <http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm>

[66] W. A. Arbaugh, W. L. Fithen, and J. McHugh, “Windows of vulnerability: A case study analysis”, *IEEE Computer,* Vol. 33, No. 12, 2000, pp. 52-59.

[67] N. Baracaldo and J. Joshi. (2013, An adaptive risk management and access control framework to mitigate insider threats. *Computers & Security*. Available: doi: 10.1016/j.cose.2013.08.001.

[68] R. Sandhu and J. Park, "Usage control: A vision for next generation access control",*Computer Network Security*, Lecture notes in Computer Science V. Gorodetsky, L. J. Popyack, and V. A. Skormin, eds., pp. 17-31, Berlin/Heidelberg: Springer 2003.

[69] K. Roy Sarkar, “Assessing insider threats to information security using technical, behavioural and organisational measures”, *Information Security Technical Report,* Vol. 15, No. 3, 2010, pp. 112-133.

[70] R. Willison, “Understanding the perpetration of employee computer crime in the organisational context”, *Information and Organization,* Vol. 16, 2006, pp. 304-324.

[71] N. L. Beebe and V. S. Roa, "Using situational crime prevention theory to explain the effectiveness of information systems security," in *Proceedings of the 2005 SoftWars Conference*, Las Vegas, NV, 2005, pp. 1-18.

[72] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. Shimeall, and L. Flynn. (2012). *Common Sense Guide to Mitigating Insider Threats, 4th Edition (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University*. Available: <http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm>

[73] T. R. Smith and J. Scott "Policing and Crime Prevention",*Crime prevention*, D. A. Mackey and K. Levan, eds., p. 82, Burlington, ma: Jones & Bartlett Publishers, 2011.

[74] J. Myers, M. R. Grimaila, and R. F. Mills, "Towards insider threat detection using web server logs," presented at the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Knoxville, Tennesse, USA, 2009.

[75] N. P. Sheppard, S.-N. Reihaneh, and P. Ogunbona, "On multiple watermarking," in *ACM Multimedia Conference workshop on Multimedia and security: new challenges* Ottawa, Ontario, 2001, pp. 3-6.

[76] J. Zhou and R. Deng, “On the validity of digital signatures”, *ACM SIGCOMM Computer Communication Review,* Vol. 30, No. 2, 2000, pp. 29-34.

[77] ISACA, *COBIT five: for information security*. USA: Information Systems Audit, & Control Association, 2012.

[78] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Roles of information security awareness and perceived fairness in information security policy compliance," presented at the 15th American Conference on Information Systems(AMCIS), San Francisco, California, 2009.

[79] A. Whitten and J. D. Tygar, "Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0," presented at the 8th USENIX Security Symposium, Washington D.C., 1999.

[80] A. Pashalidis and C. J. Mitchell, "A taxonomy of single sign-on systems",*Proceedings of the 8th Australasian Conference on Information Security and Privacy (ACISP)*, Lecture Notes in Computer Science R. Safavi-Naini and J. Seberry, eds., pp. 249–264, Wollongong, Australia: Springer-Verlag, 2003.

[81] M. Kelly. (2002, 21 September 2013). *Is single sign on a security risk?*. Available: <http://www.giac.org/paper/gsec/811/single-sign-security-risk/101711>

[82] S. Heilbronner and R. Wies, “Managing PC networks”, *IEEE Communications Magazine,* Vol. 35, No. 10, 1997, pp. 112-117.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Appendix A: Framework of Situational Crime Prevention: Towards Best Practices | | | | | |  |
| TECHNIQUES | | | | | | **No of Best Practices.** |
| Increase Efforts | *Target Hardening*  Implement strict password and account management policies and practices **(#7)** | *Control of Access to Facilities*  Institute stringent access controls and monitoring policies on privileged **(#10)** | *Screen Exits*  Close the doors to unauthorized data exfiltration **(#19)** | *Deflecting Offenders*  Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour **(#4)**  Enforce separation of duties and least privilege**.(#8)** | *Controlling Tools*  Enforce separation of duties and least privilege**.(#8)**  Develop a comprehensive employee termination procedure**(.#14)**  Filter Downloads of Illicit Tools\* | *6* |
| Increase Risk | *Extending Guardianship*  Monitor and control remote access from all end points, including mobile **(#13)** | *Assisting Natural Surveillance*  Develop a formalized insider threat program **(#16)** | *Reducing Anonymity*  Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions **(#12)** | *Utilising Place Managers*  Institute multiparty controlsβ | *Strengthening Formal Surveillance*  Institutionalize system change controls **(#11)**  Establish a baseline of normal network behaviour**(#17)** | *5* |
| Reduce Rewards | *Concealing targets*  Restrict public domain information (both internally and externally) β | *Removing Targets*  Implement Clear Desk policy and Clear Screen policiesβ | *Identifying Property*  Know your assets **(#6)** | *Disrupting Markets*  Disrupt the markets that benefit from cybercrimeβ. | *Denying benefits*  Implement secure backup and recovery processes **(#15)** | *2* |
| Reduce Precipitators | *Reducing Frustrations and Stress*  Anticipate and manage negative issues in the work environment **(#5)** | *Avoiding Disputes*  Anticipate and manage negative issues in the work environment**(#5)** | *Reducing Emotional Arousal*  Anticipate and manage negative issues in the work environment**(#5)** | *Neutralising Peer Pressure /Social Engineers*  Consider threats from insiders and business partners in enterprise-wide risk **(#1)**  Be especially vigilant regarding social media(#18)/ social engineersβ | *Discouraging Imitation*  Implement secure backup and recovery processes**(#15)** | *4* |
| Remove Excuses | *Setting Rules*  Clearly document and consistently enforce policies and controls**(#2)**  Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities**(#9)** | *Posting Instructions*  Issue rules of behavior to all users and implement banners on all systems α | *Alerting Conscience*  Issue rules of behavior to all users and implement banners on all systems α | *Assisting Compliance*  Incorporate insider threat awareness into periodic security training for all employees **(#3)**. |  | *3* |
|  | **Note:**  α Best Practices proposed by Guido and Brooks [[40](#_ENREF_40)].  β Best Practices proposed by the author. | | | | | |